Development
Of
A Model Integrated Framework of Risk Identification and Governance for Hybrid Cloud Infrastructure.

A

SYNOPSIS / RESEARCH PROPOSAL

SUBMITTED TO

VIVEKANANDA GLOBAL UNIVERSITY, JAIPUR

(Established by Act No. 11/2012 of Rajasthan Govt. Covered u/s 2 (f) of UGC Act, 1956)

THE VIVEKANANDA GLOBAL UNIVERSITY, JAIPUR

FOR THE DEGREE
OF

DOCTOR OF PHILOSOPHY

IN
(Computer Science)
By

Neeraj Kumar Dikshit
Reg. No. VGU/2016/RES/SCH/CS/0103

Faculty/Department/Subject
Faculty of Engineering and Technology
Department of Computer Science and Engineering
Computer Science – Hybrid Cloud

VIVEKANANADA GLOBAL UNIVERSITY,
RAJASTHAN – 333001

Year: 2016-17

A. Objective and Scope of the Research Investigation:

Abstract: After the practical implementation of the cloud technology across various type of Organizations Including commercial and non-Commercial organizations, it has been realized that Keeping entire IT resources and services on Public Cloud is too risky and not always a cost effective proposition.

Perhaps it's best to distribute your IT resources — and not rely on just one: IT Cloud Service, but multiple services including having Private cloud On-premises ("On-premises cloud") or Virtualized On –Premise IT Infrastructure along with Legacy IT resources.

James Kaplan, Chris Rezek, and Kara Sprague of McKinsey in their report on cloud remarked "**Having a Mixed portfolio of cloud services, as well as on-premises capabilities, may be the best way to guard Sensitive data, they suggest. This is especially important since simply "refusing to use cloud Capabilities is not a viable option for most institutions".**

Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

Hybrid cloud is particularly valuable for dynamic or highly changeable workloads.

In Nut shell, below table explains the overall benefits of Hybrid Cloud over other Cloud Models:

Table 2 :The Comparative Benefits of Different Styles Of Cloud Computing

Area	Private (on premise)	Hybrid Private (on/off premise)	Hybrid Multi-Tenant (off premise)	Public (off premise)
TCO	1.5	2.0	4.0	5.0
Security	5.0	4.5	3.5	1.5
Elasticity	1.0	3.0	4.0	5.0
Performance	4.0	5.0	5.0	2.0
Average	2.9	3.6	4.1	3.4
Standard Deviation	1.93	1.38	0.63	1.89

Source: ITCandor, November 2010

Security Risks and Challenges in Hybrid Cloud:

Hybrid cloud isn't perfect and still includes a few of security obstacles. Hence if any business maintaining a hybrid cloud, they have to keep the following Major security issues in their Mind:

1. **Absence of data redundancy:**
   Hybrid cloud is a complex system. Limited experience in identifying and managing security challenges in the cloud environment creates great risk. Cloud architects need redundancy across data centers to moderate the impact of an outage in a single data center. A lack of redundancy can become a serious security risk in hybrid cloud, specifically if redundant copies of data are not distributed across data centers.

2. Compliance :

In a hybrid cloud maintaining and demonstrating compliance are more difficult. Not only you have to ensure that your public cloud provider and private cloud are in compliance, but you also must demonstrate that the means of coordination between the two clouds is compliant.

3. Poorly constructed SLAs:

You have to be very confident that your public cloud provider can consistently meet expectations detailed in the service-level agreement (SLA). Ascertain your private cloud live up to that same SLA. If not, you may need to create SLAs based on expectations of the lesser of the two clouds and that may be your private cloud. Collect data on your private cloud's availability and performance and look for potential problems with integrating public and private clouds that could disrupt service.

4. Risk management:

It is extremely difficult to manage Information security and risk perspective of a business organization. Cloud computing (hybrid cloud in particular) uses new application programming interfaces (APIs), requires complex network configurations, and pushes the limits of traditional Security System administrators' and Solution experts ‘s knowledge and abilities. These factors introduce new types of threats.

5. Security management:

The existing security controls such as authentication, authorization and identity management should work in both the private and public cloud. But Hybrid Cloud is the combination of all modes of Cloud models integrated with Internal Virtualized Infrastructure. Hence to integrate these security protocols in hybrid environment and prove compliance could be fairly complex issue to handle.

Objective of the Study:

This research an informed assessment of the security risks and benefits of using Hybrid Cloud Computing - providing security guidance for potential and existing users of cloud computing.

Hybrid Cloud computing security is an important aspect to be evaluated and mitigation of the Same has to be reviewed since **there is no integrated framework of the Risks Identification and Governance for the Hybrid IT.** This research will highlight the key concepts of cloud security, Industry recognized various IT Security Standards/Best Practices/Frameworks and Processes .being adopted in SMEs and Enterprise Organizations as well as cloud service providers.

The purpose of this Research is to propose /develop a Model Integrated Framework of IT Security Risk Management for Hybrid Cloud Infrastructure where the focus is on Risk Identification and Governance

The objectives of this Research are following:

1) To analyze the current Hybrid Cloud and Virtualization Environment with respect to potential risks and regulatory /statutory compliance challenges.

2) Study and analyze available Standards/Frameworks/Methodologies/Best Practices for the Risks Identification, Assessment and Governance of the Hybrid Cloud and On-Premise Virtualized IT Infrastructure.

3) To establish the urgent need and requirement for An Integrated Risk Identification /Assessment and Control Framework for the Hybrid Cloud and On-Premise Virtualized IT Infrastructure .
4) To Develop and Propose the Risk Identification and Governance Framework.

5) To conclude the applicability of the Proposed Governance Framework in The Hybrid Cloud: Public, On -Premise Private Cloud, On-Premise Virtualized Infrastructure along with Legacy IT Resources.

Scope: The scope of this research study is restricted to the following:

1) To Identify and Analyze all the Standards/Frameworks/Best Practices for the overall risk identification and control to secure the Cloud and On-Premise Virtualization Infrastructure specially focusing Hybrid Cloud Infrastructure.

2) To establish the absence of an Integrated and Standard Framework for the Hybrid Cloud Risk Governance and Compliance and prove the urgent requirement of the same by the organizations and IT industry at large.

3) To Develop and propose an Integrated and Standardized Model for the Risk Identification and Governance Framework for Hybrid Cloud.

4) The Proposed framework will explain the applicability of the same in Hybrid cloud environment as well as all the other mode of cloud deployments including Virtualized IT Infrastructure.

5) The Practical Testing of this framework on different segments of organizations including Cloud Service Providers /Business Organizations and IT Solution Providers is out of the scope of this Research Study.

B. Proposed Methodology :

This proposed research study involves the study of already available various frameworks, standards and concepts related to Security, Risk Identification, Assessment and Governance for the In-Premise and /or Cloud Computing.

This involves the study of the research already done and being done for the Risk Assessment and Governance for the Cloud /In-Premise and especially for the Hybrid Cloud as well to prepare the case for the Model framework.

Underlining the gaps or limitations in these frameworks /standards and concepts when implemented in the complex Hybrid Cloud Environment for the End to End Risk Assessment and Governance is one of the motive of this study. Views and concerns from the CxOs of various organization are also required to be collected to highlight the need for a Model Integrated Risk Identification and Control Frame work.

Proposing the Model Integrated Framework for Hybrid Cloud Infrastructure is the ultimate objective of this study.

So the research methodology and approach planned for this project is explained below:

1. **The nature of the study:**

   This Study is Qualitative and Descriptive in nature as this involves the study of the Present situation of a phenomena in this case Risk Assessment and Governance in Hybrid Cloud Infrastructure. This Study can be categorized in Applied Research as well as it try to find out the solution for an existing practical problem being faced by the Organizations at large while adopting Hybrid IT approach .

2. **The purpose of the study :**

   The purpose of this study is to propose a Model Integrated Framework of Risk Identification and Governance for Hybrid IT Infrastructure which is an attempt to address the existing practical problem of inability to Measure the Risks and Devise the Control in Hybrid Cloud to by CxOs and Organizations at large to ensure the compliance and assure the stakeholders.

   As outlined above in the Research Objective section**,** the main objectives of this research Are following:

   1. To analyze the current Hybrid Cloud and Virtualization Environment and establish the need and requirement for An Integrated Risk Identification and Control Framework for the same.

   2. To Develop and Propose the Risk Identification and Governance Framework,

   3. To conclude the applicability of the Proposed Governance Framework in The Hybrid Cloud: Public, On -Premise Private Cloud, On-Premise Virtualized Infrastructure along with Legacy IT Resources.

3. The location where the study would be conducted:

The study will be conducted in Primarily National Capital Region (NCR) but not restricted to other locations within India. Google, Shodh Ganga, Shodh Gangotri and various Online Free Research Journals will be used to find out the research done and being done in the field of Risk Identification and Governance for Hybrid Cloud and other related areas.

4. Research Questions :

From the previous section i.e. Introduction Section, it is not hard to accept the fact that in the area of Hybrid Cloud, `security' is still a challenge. As long as this new paradigm does not evolve into a more secure computing platform, which users (organizations/individual) can trust, depend on and utilize in everyday work, harnessing the benefit of Hybrid Cloud is not possible.

Preliminary studies show that most of the organizations are concerned about security when considering Hybrid Cloud Infrastructure applications. There is no standard for Cloud Risk identification and Governance including the Hybrid Cloud infrastructure that has more integration and security complexities by its very design. If there are no security standards, In other words the existing Risk Assessment and Governance solutions or practices are not sufficient for the Hybrid Cloud environment.

If the existing methods are not satisfactory, there could be better ways (solutions /guidelines / practices/Frameworks) developed to improve security in Hybrid Cloud. Before developing better methods/frameworks, existing challenges and their solutions need to be identified, research question are required to be framed to know Risk challenges and mitigation strategies, specific to Hybrid cloud and the current practices followed by the different

Finally to list out solutions/practices/guidelines for handling Hybrid Cloud security issues. We need to propose the Framework/Solution/Guidelines which is integrated model for the Risk Assessment and Governance for Hybrid Cloud Infrastructure to enhance the security and ensure compliance.

To find answers for issues discussed above, the following research questions are Framed:

1. What are the security related challenges in Hybrid Cloud Model?

2. What solutions/standards/framework are present to handle security related Hybrid cloud challenges?

3. What are the issues / gaps and limitations in the available Risk Assessment and Security Standards /Frameworks for Hybrid Cloud security governance and compliance?

4. How does an organization handle the identified security challenges in Hybrid Cloud Infrastructure and feel the need for a comprehensive and standard manual or Framework for End to End Risk Identification, Assessment and Management for Hybrid Cloud?

5. Would Comprehensive Guidelines to Identify Risks and Control the same through Model Integrated Risk Assessment and Governance Framework help enhance security, reliability and compliance for Hybrid Cloud infrastructure?

5. From where the required data will be collected :

a. Collecting data from literature:

To identify which areas of Hybrid Cloud Computing Risk Analysis and Governance need more research, initially Cloud Computing challenges are found (this is done by searching the literature). Available methods for achieving this are literature review (LR) and systematic literature review (SLR).

SLR is used to find all available data relevant to a particular research area. Since the topic of Hybrid Cloud Risk Identification and Governance is a new idea, literature review and snowball sampling will be employed.

The article written by the researchers are based on scientific papers, online sources, journals etc. Snowball sampling revisits all these references used in writing an article. This in turn increases the final set of papers used to understand the problem (selected for study). Literature review using online databases involves a series of steps :

1. Identifying the keywords for the topic.
2. Creating a list of possible search terms.
3. Using search engines, electronic research journal databases to find information.
4. Modify the list of terms and repeat step 3.

b. Collecting data from real world :

Based on results of literature review and empirical study, mechanisms that are actually used in organizations to handle the security challenges identified from literature are needed to be found.

The objective here is to identify solutions/practices used in organizations. Surveys are chosen over other methods of empirical studies, as these can be simple and also easy to answer. The surveys are used to provide a quantitative or numeric description of trends opinions or attitudes. The surveys are used to gather the solutions / practices /guidelines to the challenges which have no mitigation strategies proposed (and have been repeatedly cited by many papers as a challenge).

The process of survey will be used to answer Research Question **3 and 4**, as the objective is to gather solutions/practices/standards for Risks Identification and control challenges identified through literature review.

Survey will be done on a selected group of people (who are essentially professionals working in cloud computing and are in various designations, experience levels and companies) by providing each of them with a survey questionnaire through email which has same set of questions. Since most respondents will prefer to answering questionnaire through email mode, this process of survey will suite best in saving time and effort.

Observation Method will also be used to collect the latest information about the Hybrid Cloud infrastructure Security Risks Identification and Management as it is unfolding in the real world.

6. Data Collection Method:

1. SLR (Structured Literature Review
2. Questionnaire and Surveys.
3. Observations

7. Data Sample Design: Non-Probability Sampling Approach will be followed and Snowball Sampling Method will be used as the Population Universe is too large and not fully known. Since we have selected criteria for the sample representation hence snowball sampling method is most suitable for our research.

8. The limitations and constraints:

Since this study has the objective to find out challenges in Risk Identification and Governance for the Hybrid Cloud Infrastructure which is a very recent phenomena ;a very few people and Institutions have attempted or concentrated on this burning yet very practical issue being faced by the present CxOs and organizations at large. **Therefore this study has the threat of finding very few references of existing research done or being done in this subject area.**

Based on the information gathered from literature review, surveys and observations; an analysis will be employed to develop general explanations for the research domain... This helps to identify the key concepts, terms and also resources used by other researchers. This data will be used to develop alternative designs or find out need for further research.

9. **Data Sample Size:** As per Bertaux and Bertaux-Wiame (1981) Analytic induction, the sample size between 15 to 30 is sufficient for all types of Qualitative Researches. So, I would plan to collect data from 30 sources by selective sampling method as this research requires information from the sources that are well conversant and have practical experience of the issues being faced by them in Hybrid Cloud infrastructure.

10. What time period the study would cover: The study will cover the research work done or being done in the field of security Risk Identification, Assessment and Governance related to Cloud Computing, In –Premise Cloud or Private Cloud and specifically to Hybrid Cloud Infrastructure that included In House Virtualized IT Infrastructure and existing Legacy Infrastructure . **The Time span will cover work done since 2009 till end 2017**. The result will be drawn and Solution will be proposed based on the data collected till end 2017.

11. The manner in which the report would be prepared:

The results of literature review and surveys are going to be available standards, solution guidelines/practices/ frameworks .These are going to be responses from diversified group of users and with different levels of experience.

Since the observations from the literature review may not be helpful to handle the challenges identified, Model Integrated solutions/practices/guidelines proposed for the Risk Identification and Governance for the Hybrid Cloud Infrastructure will be new to the reader. Hence a narrative analysis is employed to explain the various responses observed from the surveys.

This narrative analysis will help users (individual/organizations) to consider the possible ways to identify the Risks and Govern the Risks to mitigate the challenge of security, reliability and compliance in Hybrid Cloud Infrastructure.

C. Importance of Proposed Research Investigation/ Expected outcome :

Research problem: This is ensured that the future IT infrastructure within any organization would be Hybrid Cloud Infrastructure along with Virtualized IT Infrastructure including Legacy IT Resources within the Data Center of the Organization.

Most of the organizations have already invested huge amount in the existing IT infrastructure keeping in mind the long term Business Requirements and Supporting the Legacy applications due to the immaturity of the Cloud Technologies and Their Tested offerings in real life scenarios since the Inception of Cloud Technologies in India in late 2008.

The Private Cloud can be established on the dedicated IT Infrastructure with in the Datacenter of a Tier-3 DC Services Provider or Data Center within the organization.

The Combination of Public /Private Clouds and Virtualized IT infrastructure, Interconnectivity between them and accessibility of the same over the LAN, WAN and Internet creates a very complex IT infrastructure to be managed. Further designing safeguards against potential Risks for such a complex IT Infrastructure is extremely difficult task for any organization and especially for CxOs.

It is a great challenge for the CxOs and IT Professionals to Identify the Risks involved in such a complex environment and device a strategy to mitigate them to convince the Business Stake Holders about the security of the IT Infrastructure and Data residing on it.

Importance of the Proposed Research Work:

The Ever evolving information technologies and solutions provide organizations to meet business challenges of Stiff Competition, Cost Effectiveness, Production Efficiency, Quick and accurate decision makings and course corrections. Through the implementation of latest information technologies such as cloud computing and virtualization, an organization could become more competitive. **But appropriate and effective governance of IT Infrastructure or systems Landscape and Information data are parallel to successful operation of an organization.**

There are Lots of discrete Standards and Frameworks available for the security of the on premise IT infrastructure and few are evolving for the Cloud Infrastructure... Though there is no written standard framework for the on Premise IT Infrastructure, but as per the Best practices followed by the IT Industry across the world there is some maturity in Risk Identification and mitigation processes to be followed to secure the in premise IT infrastructure. ISO7001/7002, COBIT, ITIL, BS9977 etc. are some of the Security Risk Identification and Mitigation frameworks. Same has been extended by the organizations and IT cloud services providers to establish a security framework for the Cloud Infrastructure but there is no standard framework /manual/ reference guide for the Cloud Bases Infrastructures and services.

Hybrid cloud Infrastructure Model which is the Future of the Cloud Scenario across the world, present the greater challenge in the Risk Identification and Mitigation due to complex integration of On-Premise and On-Cloud Infrastructure and Application Interoperability issues between them.

There is a drive towards ISO security framework compliance and governance to secure the Cloud IT infrastructure from Risks. **However, a formalized and integrated governance structure and guidelines specific to Hybrid cloud computing and virtualization environment does not exist as of now.**

Because of the absence of any Standardized Risk Identification and Control Frame Work for the Hybrid IT Infrastructure, it is difficult for the CIOs/CxO/IT Managers and Network Security expert to ensure that they have Identified all the possible Risks in their Organization and adopted the best practices for the Governance and Control of those Security Risks in the Hybrid Cloud /IT Infrastructure.

This is required to ensure the Business Stake Holders about the Protection from the Potential Security Risks to the organization.
IT Industry also needs this to develop Techniques and Tools to help CIOs/CXOs/CISOs and Security Professionals in controlling the Risks in the Hybrid IT Infrastructure.

In Nut-Shell "**A Model Integrated Risk Identification and Governance Framework for Hybrid Cloud and Virtualized Infrastructure** "would provide a governance structure and guidelines to identify and evaluate Hybrid cloud computing and virtualization benefits and risks and implement controls. **The Framework will act as a Practical Manual and Guide for all the concerned entities /stake holders including CIO/CTO/IT Managers while Designing Hybrid Cloud and Virtualized environment and Devising appropriate controls with the help of policies and software tools to ensure regulatory compliances as well**

This Research work will attempt to develop a comprehensive and Integrated Model Framework for the Risk Identification and governance framework in Hybrid Cloud Infrastructure.

Expected Deliverables / A few paramount implications of the study are outlined here:

a. Findings of this study will be quite informative and useful for both general public and companies indulge in cloud technology. They can understand the dimensions reflecting benefits and risk of Hybrid Cloud computing and impact of all these factors on an enterprise.

b. Findings of this study will inform that it is worthwhile for an enterprise to take note of the IT Industry at large involved in to the business of providing solutions around the Cloud Technologies , Cloud Security solutions , Information Security Monitoring and Mitigation Products , will have to align their Product Road Maps as per the Risks , Their Governance challenges and suggested Mitigations for the same in Hybrid Cloud Infrastructure as provided in the Proposed Model Integrated Risk Identification and Governance Framework for the Hybrid cloud Infrastructure.

c. This study will provide the Risk Identification and Governance Framework for The CXOs and Industries at Large that will influence any enterprise using or planning to use Public Cloud along with the existing Legacy IT Infrastructure, In Premise Private cloud or Virtualized It Environment computing technology in India or abroad.

d. The final deliverable after this research will be the answers to the Research Questions as explained above in the **Framing Research Questions Section** and **a Model Integrated Framework for the Risk Identification and Governance for the Hybrid Cloud infrastructure. This Framework could be used as a readily available Manual/Guide/Handbook to be referenced that provide all the relevant aspects of Hybrid Cloud Risk Identification and Governance as well as attempt to suggest Software Tools (wherever possible based on the availability and suitability) to help all the concerned stake holders of current or prospective Hybrid Cloud Implementations.**

D. Review of the work related to the field of Research- already done on the subject -Present and Past Status:

As per **Gartner Report on Market Trends: "Cloud Adoption Trends Favor Public Cloud with a Hybrid Twist" Published dated 04 August 2016 with ID: G00294424:**
"Cloud computing has become today's most common technology buzzword. Despite the promises of cloud computing to decrease computing implementation costs and deliver computing as a service, which allows clients to pay only for what they need and use, **cloud computing also raises many security concerns**."

Another very important observation made by this Gartner report is: "**Hybrid Cloud Computing is the Future of the Cloud Computing where Internal Private Cloud (Enterprise Wide Virtualized Environment) and Hosted Private Cloud will be used significantly ".**

Following Marketing Trends are presented by the Gartner Report on Cloud Adoption and the Preferred Model for the future:

- **Market Trend No. 1: Rapid Growth of Cloud Adoption Continues**, Trending Toward Public Cloud
  - Organizations Using Cloud Almost Always Have a "Cloud First" Strategy
  - Forty Percent of IT Spending Is Allocated to Cloud, With Increases Expected
  - IT Modernization Leads as the Top Driver for Public Cloud Adoption
  - **Security and/or Privacy Concerns Is the Top Inhibitor to Public Cloud Adoption**
- **Market Trend No. 2: Hybrid Cloud Scenarios Will Dominate**
  - Organizations Use a Variety of Cloud Models
  - **Hybrid Cloud Usage Will Increase**
  - **The Use of Internal Private Cloud and Hosted Private Cloud Will Increase**
- **Market Trend No. 3: The Lines Are Blurring Between Cloud Service Types**

- **Public Cloud Services Must Reliably Meet an Increasingly Diverse Set of Requirements**

So this is ample clear that Hybrid Cloud with the increased usage of internal private cloud and hosted private cloud along with need based usage of public cloud would create a very complex environment to manage especially in terms of Risk Assessment and Governance along with regulatory and statutory compliances.

According to a survey to rank cloud computing challenges and issues, conducted by the **International Data Corporation (IDC), security was ranked as the major concern in a cloud computing environment** [7]

Most popular risk assessment standards, such as ISO27005, NIST SP800-30, and AS/NZS 4360, assume that an organization's assets are fully managed by the organization itself and that all security management processes are imposed by the organization. These assumptions, however, do not apply to cloud computing environments. [6]

Hybrid Cloud Security is more complex than cloud security and In Premise security hence need different approach.

Over the last one decade, numerous of documents /articles and research works have been written or published informing about various risks , providing ad-hoc guidance and control checklists to be referred while considering cloud computing infrastructure deployment in any organization or setup.

Most of these Documents and Research works are deeply concerned with and focused on security aspects in cloud infrastructure but very less concerned across the spectrum about the IT Risks involved where a comprehensive Framework for Risk Assessment and Governance is needed.

The International Organization for Standardization (ISO) is attempting on the development of various standards that aim to formally address the risk management aspect of cloud computing infrastructure and services.

Since the risk profile for migration to cloud services is not fixed and certain due to the continuous maturity of the existing and frequent announcement of new cloud services by various Cloud Services Providers across the world, it is very difficult to map risks and their governance comprehensively.

Risk Governance is a challenge as there is no standard definition and process for the Risk Assessment. [1] Different standards take different approaches to the processes of **Information Security Risk Assessment (ISRA)**. [1]

For instance, SP800-30, ISO 27001 and ISO 27005 provide the slightly different definitions and procedures for Information Security Risk Assessment (ISRA). [1] Of these three standards, ISO 27005 provides more accurate definitions for each stage of the ISRA process. [1]

In this sense, it is important to come to a common understanding of the processes and terminology to simplify research in this area. [1]

In, 2009, the European Network and Information Security Agency (ENISA) produced a document titled 'Cloud Computing: Benefits, Risks and Recommendations for Information Security'. This document collates 35 types of risk identified by 19 contributors, and identifies eight top security risks based on ENISA's view of indicative likelihood and impact.

In March 2010, the Cloud Security Alliance (CSA) published 'Top Threats to Cloud Computing V1.0', which includes the top seven threats as identified by its members.

In April 2011, the Open Web Application Security Project (OWASP) released a 'pre-alpha list' of its top 10 cloud Security risks derived from a literature review of other publications and sources...

In May 2011, the National Institute of Standards and Technology (NIST) released a draft titled 'Cloud Computing Synopsis and Recommendations (Special Publication 800-146)', which provides a deep analysis of risks in the Cloud Computing, but no **coherent framework was produced or proposed.**

In ISACA Journal Vol 5, 2012, Article: Cloud Risk—10 Principles and a Framework for Assessment
Written by David Vohradsky, a collated table of 10 Top cloud risks and their importance in terms of overall impact identified by CSA, OWASP and ENISA has been given.

This compilation clearly highlighted that Cloud Risk is not a traditional Security and Risk issue but it is far more complex issue to be tackled as various points of failures or risks are not in your direct control.

Figure 1 gives a comparison of the top types of risk identified by the CSA, OWASP and ENISA showing the variation in both content and ranking:

Figure 1—Ranking Comparison of Top Risks

Risk	CSA Ranking	OWASP Ranking	ENISA Ranking
Abuse and nefarious use of cloud computing—Due to the often anonymous nature of some cloud services, they attract use by criminal elements.	1	-	-
Insecure interfaces and application programming interfaces (APIs)—Due to the open nature of cloud services, interfaces and APIs often use anonymous access, cleartext authentication or content transmission.	2	-	-
Malicious insiders—Cloud providers offer little transparency into their supply chain, human resources, security management or incident management processes.	3	-	8
Share technology (multitenancy/isolation) risk—One tenant can deliberately or inadvertently interface with the security or performance of another tenant.	4	7	3
Data ownership (governance) and accountability—Data ownership, encryption, transmission, operational failure, data disposal/data deletion and availability are all challenges in a cloud environment.	5	1 (Ownership) 5 (Data loss)	1 (Ownership) 7 (Data deletion)
Account or service hijacking (including management interface)—Using social engineering, phishing, fraud or vulnerability exploits, attackers can compromise confidentiality, integrity and availability.	6	9	5
Unknown risk profile—Cloud providers offer little transparency into compliance, security procedures, configuration management, logging and monitoring, leaving customers with an unknown risk profile.	7	8	-
User identity federation—Use of multiple cloud offerings can result in islands of identities that need to be maintained.	-	2	-
Regulatory compliance—Regulatory environments differ across countries and regions, particularly with regard to privacy.	-	3	4
Business continuity and resilience—These are delegated to the cloud provider and may not be appropriate. Pricing pressure results in commoditisation that de-emphasises this.	-	4	-
Service and data integration/protection—Data handling or data protection fails during transmission between end user and data centre, or between federated clouds.	5 (CSA covers both this risk and the other data risk noted previously.)	6	6
Non-production environment exposure—A cloud provider is used for design, development and test activities, which are typically less controlled.	-	10	-
Lock in—Minimal tools, procedures, standards or interfaces are in place to guarantee data, application, service or business process portability.	-	-	2

Source: ISACA Journal Vol 5, 2012, Article: Cloud Risk—10 Principles and a Framework for Assessment
By David Vohradsky, CGEIT, CRISC

In the domain of Risk Assessment and Governance Framework most authors try to improve the whole process of ISRA by following different standards like ISO 27005 and NIST SP800-30. [1]

CSA" security guidance for critical areas of focus in cloud computing v3.0 "highlight areas of concern for cloud computing to address both the strategic and tactical security 'pain points' within a cloud environment that can be applied to any combination of cloud service and deployment model. **It identified 13 Major Risks** that are outside the Cloud Architecture that are very critical for the overall security and reliability of any type of cloud deployments. **The top 5 Risks** are related to: **1. Governance and Enterprise Risk Management; 2. Legal Issues: Contracts and Electronic Discovery; 3. Compliance and Audit; 4. Information Management and Data Security and 5. Portability and Interoperability**

In this Guide CSA , attempted to provided broad guidelines to secure the 13 identified risks applicable in all types of Cloud Models; but do these are compliant with more accepted security standards like ISO 27005/ COBIT/NIST SP 800-30 and how to prove the compliance is not provided.

Cloud Standards Customer Council (CSCC) in its **"Practical Guide to Hybrid Cloud Computing"** recognized that "there **is need for a comprehensive framework for the Hybrid Cloud Environment**". [16]

In this Guide , it is highlighted that for a successful implementation of Hybrid Cloud **" both strategic and tactical activities for decision makers implementing hybrid cloud solutions are recommended that covers all the essential technical considerations for hybrid cloud deployment including integration, connectivity, governance, management, security and privac**y."[16]

Prescriptive guidance for successful implementation of Hybrid Cloud has been provided in this guide but how exactly these should be implemented and security compliance must be ensured as per various standards and risk assessment methods and procedures is still a challenge for the CxOs, Security Experts, Hybrid Cloud Solution Providers and Cloud Service Providers. [16]

E. Research Gaps identified in the proposed field of investigation - Based on review :

Hybrid Cloud Risk Governance is a challenge as there is no standard definition and process for the Risk Assessment.

In this sense, it is important to come to a common understanding of the processes and terminology to clarify research in this area. [1]

Different standards take different approaches to the processes of Information Security Risk Assessment (ISRA). [1]

Many standards exist to guide the process of Risk Assessment and Governance, particularly in the field of Information Security. [1]

Cloud Security is considered as the Extension of the on premise IT security perimeter over the internet. [5] But it has been proved that Cloud Risk Analysis, evaluation and assessment requires more detailed and complex approach as lots of functions are not in the direct control of the user organization and dependent on the security governance program of the Cloud Service Providers.

In the Area of Overall Security and Risk Management in Cloud Infrastructure, **Most of the efforts have been made mainly in improving the security mechanism within the Cloud Architecture** itself by Researchers and Various associations and bodies working towards the development of

security frameworks in cloud infrastructure. **But not much has been done in the Area of Information Security Risk Assessment and its Governance**.

In the Research domain of Risk Assessment and Governance Framework for Cloud infrastructure and services; most of the researchers and authors have tried or trying to improve the whole process of ISRA by following different standards like COSO , ITIL V3.0, ISO 27005 and NIST SP800-30. [1]But there is no unified and integrated Model of Risk Assessment and Governance for In-House Virtualized Infrastructure and all types of Cloud Models i.e. Public, Private and Hybrid clouds.

Hybrid Cloud Security is even more complex than cloud security and In Premise security hence need different approach towards the Risk Identification, Assessment and Governance.

After Reviewing all the referenced literatures as well lots of other articles published in various Professional magazines and on internet; it is established that there is a requirement of **a Model Integrated Risk Assessment and Governance Framework for the Hybrid Cloud.**

Also this is discovered that there not much of the work has been done in understanding the risks and governance in a hybrid cloud scenario with increasing usage of In house Private Cloud / Enterprise wide Virtualized IT Infrastructure and Hosted Private Cloud. There is no published framework or manual available that should provide a single consolidated Practical Guide for Risk Identification , Risk Assessment , Risk Governance and Risk Mitigation Plan for the Hybrid Cloud Infrastructure .This is extremely needed by the concerned to increase the reliability in Hybrid Cloud Infrastructure and provide the assurance and compliance to the concerned stake holders

F. Chapter wise details of Proposed Research Investigation Ph.D. Thesis:

Chapter 1 – Background Introduction.

Introduction and Background about the Virtualization, Cloud and Risk Governance is provided in this chapter along with the description of Research problem /objectives and approach.

Chapter 2 – Virtualization and Cloud –Terminologies and Definitions.

All the Relevant Terms, Terminologies and Definitions are listed in this chapter to help readers understand the subject matter properly.

Chapter 3 – Research Design and Methodology Adopted.

In this section Research Design and Methodology adopted to conduct this research is explained. Research, Data collection methods and Analysis techniques used will be explained in this chapter. Overall this chapter describes how this research has been conducted.

Chapter 4 – Why Risk Identification, Assessment and Governance Framework for Hybrid Cloud is needed?

This Chapter contains the background and the justification for this research work that attempts to develop a Model Risk Identifications and Governance Framework for the Hybrid Cloud.

Chapter 5 – Proposition for the Development of a Model and Integrated Risk Identification and Governance Framework for Hybrid Cloud.

This chapter defines the objectives and provides a suggestion for the development of the proposed framework. This chapter explains the Structure of the governance framework for cloud computing and virtualization and Identification of the proposed framework components. Integration of the identified components into a functional structure and finally Method to apply the proposed Framework.

Chapter 6 – Cloud computing and virtualization benefits.

This chapter presents a list of cloud computing and virtualization benefits and explains them.

Chapter 7 – Risks in Virtualization and Cloud computing.

The Risks in Virtualization and cloud computing risks, obtained through the detailed analysis of the literature is summarized and discussed in section.

Chapter 8 – Existing Standards and Frameworks for Cloud computing and virtualization Risk Assessment and Controls.

This chapter describes the existing risk control standards, frameworks and guidelines and intends to map the controls (from these standards, frameworks and guidelines) to the list of cloud computing and virtualization risks identified .

Chapter 9 – Development of Benefit, Risk and Control Identification and Assessment Policies.

In this chapter the guidelines to identify and evaluate cloud computing benefits, risks and controls are developed. These guidelines, together with the lists of benefits, risks and controls developed earlier complete the requirement for the development of the Hybrid Cloud Risk identification and Control Framework components.

Chapter 10 – Model Integrated Risk Identification and Governance Framework for Hybrid Cloud.

This chapter presents the overall Model Integrate Risk Identification and Governance Framework for Hybrid Cloud based on the integration of the identified components into a functional structure and the development of a method (guidelines) to perform an assessment of a cloud and/or virtualized environment.

Chapter 11 – Validation and verification of the Hybrid Cloud Risk Governance Framework.

This chapter describes the validation and verification of the Framework.

The outcome of a case study conducted to evaluate the Framework. The validation is done through illustrating the applicability of the Framework using a case study, while the verification is done against a metrics .

Chapter 12 – Research Conclusion.

Research conclusion and Further Research Suggestions will be given here.

Chapter 13-- References.

Research References are given here.

G. Expected duration of the investigation (Year wise schedule):

As explained in the research methodology section of this Research Outline Document, This proposed research study will cover the research work done or being done in the field of Risk Identification, Assessment and Governance related to Cloud Computing and specifically to Hybrid Cloud Infrastructure that includes In-House Virtualized IT Infrastructure / Private Enterprise wide Cloud /Existing Legacy Infrastructure as well as balanced mix of Public Cloud services.

The expected duration of the investigation will be Beginning 2017 Time span will cover work done since 2009 till end 2017. The result will be drawn and Solution will be proposed based on the data collected till end 2017.

Following is the Expected Investigation Schedule:

Feb 2017 to Oct 2017: 9 Months Approx.

a. The Analysis of all the research works, Standards and Frameworks related to Risk Analysis and Governance for Cloud will take approx. 9 months.
b. Publication of one Research Article in a reputed International Journal related to Computer Science and Engineering
c. Publication of one Research Article in Indian Journal related to Computer Science and Engineering

Nov 2017 to March 2018: 3 Months Approx.

a. Based on the Analysis, Surveys will be conducted and Observations are recorded.
b. Compilation and Analysis of the Surveys /Observations. Results Drawn.
c. Publication of the Survey results in a reputed International Journal related to Computer Science and Engineering

April 2018 to Dec 2018: 9 Months Approx.

a. Development of the Model Integrated Risk Identification and Governance Framework for Hybrid Cloud.
b. One Live Case Study to Test the effectiveness of the Model Developed Framework through the Feedbacks received. Dry Run Method would be used to prove the concept.
c. Publication of the Case Study Results in an International Journal related to Computer Science and Engineering.

Jan 2019 to March 2019: 3 Months Approx.

a. Preparation of the Final Research Thesis Report.
b. Publication of the Research Thesis on Shodh Ganga after approval by the Research Guide and The University.

H. Facilities available for the investigation at scholar end and facilities required on campus:

I have following facilities for the Investigation which is sufficient for the Research work:

a. Laptop
b. Internet Broadband Connectivity
c. Access to CIO and Industry Forums through LinkedIn, CIO Groups, Research Groups and Personal contacts.

No facilities are required at the University Campus.

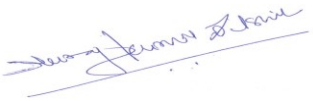
I. Bibliography :

1. ISACA Journal Vol 5, 2012, Article: Cloud Risk—10 Principles and a Framework for Assessment By David Vohradsky, CGEIT, CRISC
2. ENISA: Critical Cloud Computing, European Network and Information Security Agency (2012).
3. ISO/IEC 27005. Information security risk management (2008).
4. ENISA, Inventory of Risk Management / Risk Assessment Methods and Tools, European Network and Information Security Agency, (2005).
5. ENISA: Procure Secure: A guide to monitoring of security service levels in cloud contracts, European Network and Information Security Agency (2012).
6. NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems, National Institute of Standard and Technology U.S. Department of Commerce, (2002).
7. NIST Special Publication 800-37: Guide for Applying Risk Management Framework to Federal Information Systems, National Institute of Standard and Technology U.S. Department of Commerce, (2010).
8. ENISA: Cloud Computing: Benefits, risk and recommendation, European Network and Information Security Agency (2009).
9. NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations, National Institute of Standard and Technology U.S. Department of Commerce, (2012).
10. Vohradsky, D.: Cloud Risk – 10 Principles and a Framework for Assessment, ISACA Journal volume 5 (2012).
11. NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information System and Organizations, National Institute of Standards and Technology U.S. Department of Commerce, (2011).
12. NIST Interagency Report 7756: CAESARS Framework Extension: An Enterprise Continuous Monitoring Reference Model (Second Draft), National Institute of Standard and Technology U.S. Department of Commerce, (2012).
13. Brotby, W. K.: Information Security Management Metrics: A Definitive Guide to

14. ISBN: 978-0-9891305-1-6 ©2013 SDIWC 66Effective Security Monitoring and Measurement, Taylor & Francis, (2009).
15. Philips, M.: Using a Capability Maturity Model to Derive Security Requirements, SANS Institute, (2003).
16. ISACA: The Risk IT Framework, (2009).
17. NIST Special Publication 800-145: The NIST Definition of Cloud Computing, National Institute of Standard and Technology U.S. Department of Commerce, (2011).
18. Annamalai, N.: Information Security Guidelines for Organizations intending to adopt Cloud sourcing (Master Thesis), Department of Computer and System Sciences University of Stockholm and Royal Institute of Technology, Sweden, (2012).
19. Karokola, G.: A Framework for Securing eGovernment Services (PhD Thesis), Department of Computer and System Sciences Stockholm University, Sweden, (2012).
20. BERTAUX (1981, p.35)
21. L. Pan & A. Tomlinson, Int. J. of Safety and Security Eng., Vol. 6, No. 2 (2016) 270–281
22. NIST, SP 800-30, Guide for Conducting Risk Assessments, 2012.
23. ISO, 27001:2005, Information technology - security techniques - information security management systems - requirements. International Organization for Standardization, 2005.
24. ISO, 27005:2011, Information technology-security techniques-information security risk management. International Organization for Standardization, 2011.
25. Saleh, M.S. & Alfantookh, A., A new comprehensive framework for enterprise information security
26. Albakri, S.H., Shanmugam, B., Samy, G.N., Idris, N.B. & Ahmed, A., Security risk assessment framework for cloud computing environments. Security and Communication Networks, 2014.
27. CSCC: Interoperability and Portability for Cloud Computing: A Guide. http://www.cloud-council.org/resource-hub.htm#interoperability-and-portability-for-cloudcomputing-a-guide
28. ISO/IEC 17789: Cloud Computing Reference Architecture. http://standards.iso.org/ittf/PubliclyAvailableStandards/c060545_ISO_IEC_17789_2014.zip
29. CSCC: Practical Guide to Cloud Service Agreements V2.0. http://www.cloud-council.org/resource-hub.htm#practical-guide-to-cloud-service-agreementsversion-2
30. CSCC: Security for Cloud Computing: 10 Steps to Ensure Success. http://cloud-council.org/resource-hub.htm#security-for-cloud-computing-10-steps-to-ensuresuccess
31. CSCC: Migrating Applications to Public Cloud Services: Roadmap for Success. http://cloud-council.org/resource-hub.htm#migrating-applications-to-public-cloud-services
32. http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf
33. NIST Cloud Computing Security Reference Architecture https://www.**nist**.gov/document-4641
34. Governance Considerations for the Cloud - NIST - The Security. https://scap.**nist**.gov/events/2009/itsac/presentations/day3/Day3_**Cloud**_Ritchey.pdf
35. CSA Guidance V2.16 - Cloud Security Alliance https://**cloud**securityalliance.org/csaguide.pdf

36. Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide Published by Santa Fe Group, Oct 2010 Copy Right with The Shared Assessments Program.
37. Enterprise Risk Management for Cloud Computing – Coso www.coso.org/documents/**Cloud**%20Computing%20Thought%20Paper.pdf
38. Enterprise Risk Management Integrated framework for Cloud Computing www.ijana.in/papers/V5I3-5.pdf
39. A Proposed Risk Management Framework For Cloud Computing Environment IJCSIS) International Journal of Computer Science and Information Security,Vol. 14, No. 8, August 2016.
40. Gartner Report Market Trends: Cloud Adoption Trends Favor Public Cloud With a Hybrid Twist **Published:** 04 August 2016 **ID:** G00294424 www.gartner.com/doc/3396633/market-trends-cloud-adoption-trends
41. CC: Practical Guide to Cloud Computing. http://cloud- council.org/resource-hub.htm#practical-guide-cloud-computing-v2
42. SO/IEC 17788: Cloud Computing Overview and Vocabulary. http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip
43. IT Controls and Governance in Cloud Computing Jack D. Becker & Elana Bailey (2014 AMCIS Proceedings forthcoming)
44. CSA SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
45. Does A Hybrid Cloud Require Hybrid Security? By Danelle Au on July 15, 2013 http://www.securityweek.com/does-hybrid-cloud-require-hybrid-security
46. CSCC : Practical Guide to Hybrid Cloud Computing Feb 2016
47. White Paper : VMware/Bluelock : Security in the Hybrid Cloud : Putting Rumors to Rest *ww2.frost.com/.../Whitepaper-VMware_Bluelock_Security_In_The_Hybrid_Cloud.pdf*
48. IJCET : Security Risks in Cloud Computing: A Review Somayyeh Jafarpour and Ammar Yousefi 15 July 2016, Vol.6, No.4 (Aug 2016) http://inpressco.com/category/ijcet
49. Private & Hybrid Cloud: Risk, Security and Audit Scott Lowry, Hassan Javed Vmware Inc. 2012 http://www.theiia.org/chapters/pubdocs/79/audit_and_security_of_private_and_hybrid_clouds_iia_web.pdf
50. Pulse Secure : 17 Hybrid Cloud Security threats and how to secure them https://www.pulsesecure.net/lp/hybrid-cloud-security-threats

Name of Scholar: Neeraj Kumar Dikshit

Signature: 

Date: 16/1/2017